(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020020072618 A
(43)Date of publication of application: 18.09.2002

(21)Application number: 1020010012532
(22)Date of filing: 12.03.2001

(71)Applicant: INSTITUTE INFORMATION TECHNOLOGY ASSESSMENT SEVOI CO., LTD.

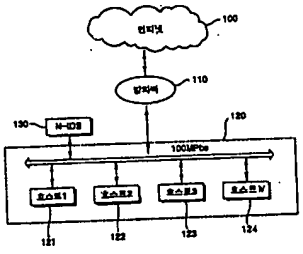
(72)Inventor: CHOI, GYEONG HUI
JUNG, GI HYEON

(51)Int. Cl G06F 15/00

(54) NETWORK BASED IDS

(57) Abstract:

PURPOSE: A network based IDS(Intrusion Detection System) is provided to enhance a packet catch performance by catching a small size packet in a high speed network without a loss and to fast and exactly detect the misuse and the abnormal activity in the network.



CONSTITUTION: The system comprises an intrusion detect sensor(130) detecting the misuse through the pattern matching after collecting the packets by connecting to the network, and an intrusion detect server generating a normal profile for each source by receiving the packets collected by the intrusion detect sensor and detecting the abnormal activity. The intrusion sensor includes a packet collecting and distributing part collecting and distributing the packet from the network, a pattern matching part detecting the intrusion by comparing the packet transferred from the packet collecting and distributing part with the previously stored pattern, a packet filtering and dissembling part dissembling the packet from the pattern matching part, and a distributing part for transferring the data from the packet filtering and dissembling part to the intrusion detect server.

Legal Status

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. 7
G06F 15/00

(11) 공개번호 특2002-0072618
(43) 공개일자 2002년09월18일

(21) 출원번호 10-2001-0012532
(22) 출원일자 2001년03월12일

(71) 출원인 (주)세보아
경기도 수원시 팔달구 원천동 28-25 화원빌딩 4층
정보통신연구진흥원
대전광역시 유성구 어은동 52번지

(72) 발명자 정기현
경기 수원시 권선구 권선동 1267 벽산한성아파트 809-1106
최경희
경기 수원시 팔달구 매탄1동 139-24

(74) 대리인 진천웅
조현실

심사청구 : 없음

(54) 네트워크 기반 침입탐지 시스템

요약

본 발명은 네트워크상에서 이루어지는 비정상적인 행위, 오용, 및 남용을 감시하기 위한 네트워크 기반 침입탐지시스템(network based IDS)에 관한 것이다. 이러한 본 발명은 망에 접속되어 패킷을 수집한 후 패턴매칭을 통해 오용을 탐지하는 침입탐지 센서; 및 상기 침입탐지 센서로부터 수집된 패킷을 수신하여 각 소스별 정상 프로파일을 생성하고 비정상 행위를 탐지하는 침입탐지 서버를 구비하고, 침입탐지 센서는 망으로부터 패킷을 수집하여 분배하는 패킷수집 및 분배부와; 미리 패턴을 저장하고 있다가 상기 패킷 수집 및 분배부로부터 전달된 패킷과 비교하여 침입을 감지하는 패턴 매칭부; 상기 패턴 매칭부로부터 전달된 패킷을 분해하는 패킷 필터링 및 분해부; 및 상기 패킷 필터링 및 분해부로부터 전달된 데이터를 상기 침입탐지 서버로 전달하기 위한 분배부로 이루어진다.

본 발명에 따른 네트워크 기반 침입탐지 시스템은 하드웨어 기반의 패턴 매칭을 이용하므로 고속망에서 작은 사이즈의 패킷도 상실(loss)하지 않고 캐쳐할 수 있으므로 패킷 캐쳐 성능을 100% 에 가깝게 향상시킬 수 있고, 이에 따라 망에서의 오용 탐지 성능과 비정상 행위를 신속 정확하게 탐지할 수 있는 잇점이 있다.

대표도

도 2

색인어
침입탐지, 해커, 패턴매칭

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 침입탐지 시스템을 설명하기 위해 도시한 도면,

도 2는 본 발명에 따른 침입탐지 시스템의 구성을 도시한 블럭도이다.

*도면의 주요부분에 대한 부호의 설명

100: 인터넷110: 방화벽 시스템

120: 내부망121~124: 호스트 시스템

130: 침입탐지시스템

200: 침입탐지 센서210: 패킷 수집 및 분배부

220: 제1 버퍼링부230: 패턴 매칭부

240: 패킷 필터링 및 분해부250: 제2 버퍼링부

260: 분배부270: IDS망

280-1~280-n: 침입탐지 서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크상에서 이루어지는 비정상적인 행위, 오용, 및 남용을 감시하기 위한 침입탐지시스템(IDS: Intrusion Detection System)에 관한 것으로, 더욱 상세하게는 네트워크를 통해 전송되는 패킷의 캡쳐성능을 향상시킨 네트워크 기반 침입탐지시스템(network based IDS)에 관한 것이다.

최근들어, 퍼스널 컴퓨터의 급속한 보급과 인터넷의 사용이 일반화되면서 전자상거래, 전자화폐, 전자메일 등 다양한 전자 비지니스가 생활의 기본 수단으로 발전하고 있고, 이에 따라 해커의 불법침입, 컴퓨터 바이러스의 유포, 프라이버시 침해 등 정보화의 역기능이 사회적 문제점으로 대두되고 있다.

이러한 문제점을 해결하기 위해 전산망 보안기술로서 가상사설망(VPN: Virtual Private Net), 방화벽(Firewall), 침입탐지시스템(IDS:Intrusion Detection System) 등이 널리 연구되고 있다. 널리 알려진 방화벽(Firewall)은 외부로부터 내부망을 보호하기 위한 기술로서 외부의 불법침입으로부터 내부의 정보자산을 보호하고, 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어 및 소프트웨어를 총칭한다. 따라서 방화벽은 통상 인터넷과 내부망

의 경계부분에 존재하여 정보의 흐름을 통제하는 기능을 하며, 네트워크 트래픽의 흐름을 가로막아 트래픽의 속도를 지연시키는 문제점이 있다. 침입탐지시스템(IDS)은 내부망이나 호스트에 위치하여 침입의 패턴 데이터베이스와 전문가 시스템을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하여 침입을 탐지하는 기술이다. 따라서 방화벽과 침입탐지시스템을 이용하면 침입차단에 실패하더라도 피해를 최소화하고, 네트워크 관리자 부재시에도 해킹에 적절히 대응할 수 있다.

그런데 종래의 침입탐지시스템(IDS)은 소프트웨어로 구현되어 네트워크를 통해 전달되는 패킷을 모두 캐취하지 못해 탐지 성능이 떨어지는 문제점이 있다. 특히, 종래방식에 따르면 패킷 사이즈가 작을 경우에는 패킷 캡쳐 성능이 약 30 % 이하로 떨어지는 것으로 알려져 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점을 해결하기 위하여 고속망에서도 패킷 캡쳐 성능을 대폭 향상시킬 수 있는 네트워크 기반 침입 탐지시스템을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위하여 본 발명은, 망에 접속되어 패킷을 수집한 후 침입을 탐지하는 네트워크 기반 침입탐지시스템에 있어서, 상기 망에 접속되어 패킷을 수집한 후 패턴매칭을 통해 오용을 탐지하는 침입탐지 센서; 및 상기 침입탐지 센서로부터 수집된 패킷을 수신하여 각 소스별 정상 프로파일을 생성하고 비정상 행위를 탐지하는 침입탐지 서버를 구비하는 것을 특징으로 한다.

그리고 본 발명에 따른 상기 침입탐지 센서는 망으로부터 패킷을 수집하여 분배하는 패킷수집 및 분배부와; 미리 패턴을 저장하고 있다가 상기 패킷 수집 및 분배부로부터 전달된 패킷과 비교하여 침입을 감지하는 패턴 매칭부; 상기 패턴 매칭부로부터 전달된 패킷을 분해하는 패킷 필터링 및 분해부; 및 상기 패킷 필터링 및 분해부로부터 전달된 데이터를 상기 침입탐지 서버로 전달하기 위한 분배부를 포함하는 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 자세히 설명하기로 한다.

도 1은 본 발명에 따른 침입탐지시스템을 설명하기 위해 도시한 도면이다. 도 1을 참조하면, 내부망(120)이 방화벽(110)을 통해 인터넷(100)에 접속되어 있고, 내부망(120)에는 다수의 호스트들(121~124)이 LAN으로 연결되어 있다. 그리고 고속으로 전송되는 패킷들을 감시하기 위한 침입탐지시스템(130)이 내부망(130)에 연결되어 있다. 본 발명의 실시예에서 내부망은 100Mbps의 고속 이더넷망이고, 통상 이더넷에는 다수의 호스트들과 터미널, 네트워크 자원들이 연결되어 있다.

개방성을 특징으로 하는 인터넷(100)은 TCP/IP 프로토콜에 따른 패킷을 통해 데이터가 전달되고, 인터넷(100)을 통해 내부망으로 전달되는 패킷들은 일차 방화벽(110)을 통해 필터링된 후 내부망(120)으로 들어오고, 내부망(120)에서 전달되는 모든 패킷들은 본 발명에 따른 네트워크 기반 침입감지시스템(130)에 의해 감시된다.

일반적으로 침입탐지 시스템은 크게 데이터수집 단계, 데이터 가공 및 축약단계, 침입분석 및 탐지 단계, 보고 및 대응 단계의 4단계 구성요소를 갖는다. 데이터수집 단계는 침입시스템이 대상시스템에 제공하는 컴퓨터 통신에 사용되는 패킷등과 같은 탐지대상으로부터 생성되는 데이터를 수집하는 감사데이터 수집단계로서, 호스트 기반에서는 호스트의 사용 내역이 기록되어지는 자체의 로그파일이 있으므로 이 파일들로부터 관련 데이터를 수집하고, 네크워크 기반에서는 네트워크를 통해 전달되는 모든 패킷들을 캐취하여 수집한다. 수집된 일련의 감사데이터들은 데이터 가공 및 축약단계에서 침입판정이 가능하도록 의미있는 정보로 변환시키고, 분석 및 침입탐지 단계에서는 이를 분석하여 침입 여부를 판정한다.

침입탐지 단계는 시스템의 비정상적인 사용에 대한 탐지를 목적으로 하는지, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입탐지를 목적으로 하는지에 따라 비정상 행위 탐지기술과 오용 탐지기술로 구분된다. 보고 및 대응 단계에서는 침입탐지 시스템이 시스템의 침입여부를 판정한 결과 침입으로 판단된 경우, 이에 대한 적절한 대응을 자동으로 취하거나 보안관리자에게 침입사실을 보고하여 보안관리자에 의해 조치를 취하게 한다.

이러한 침입탐지 시스템은 침입모델을 기반으로 하는 분류방법과 침입탐지를 위한 데이터 획득위치 즉, 데이터 소스를 기반으로 하는 분류방법 등이 있는데, 침입모델을 기반으로 분류하면 비정상 행위 탐지방법과 오용 탐지방법으로 구분된다. 데이터 소스를 기반으로 분류하는 방법은 단일 호스트로부터 생성된 감사데이터를 침입탐지에 사용하는 호스트 기반과, 네트워크에 연결된 여러 호스트로부터 생성된 감사데이터를 수집하여 침입을 탐지하는 다중 호스트 기반, 그리고 네트워크의 패킷 데이터를 수집하여 네트워크 침입을 탐지하는 네트워크 기반으로 분류할 수 있다.

여기서, 오용침입이란 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있는 공지된 공격형태를 말한다. 오용탐지 방법에서는 이와 같은 공지된 모든 침입행위를 패턴이나 시그네쳐의 형태로 설정한 후 동일한 방법의 침입을 기설정된 패턴이나 시그네쳐를 통해 탐지하는 방법이다. 이와 같이 오용침입 탐지방법은 기존의 침입기법들에 대한 패턴이나 시그네쳐를 통해 탐지하는 방법이므로, 기존의 침입기법들에 대한 패턴이나 시그네쳐를 얼마나 잘 생성하느냐가 아주 중요하다. 이 때, 생성된 패턴이나 시그네쳐들은 정확히 침입인 것만을 구별해낼 수 있도록 만들어져야 하는데, 그렇지 않을 경우에는 긍정적 결함(false positive)과 부정적 결함(false negative)이 발생할 수 있다. 이 방법은 알려져 있는 많은 침입들을 탐지해낼 수 있지만, 알려지지 않은 방법을 사용하는 침입은 탐지할 수 없는 단점이 있다. 그리고 오용침입 탐지방법은 공지된 침입정보를 어떻게 구성하느냐에 따라 전문가시스템, 시그네쳐분석, 페트리넷, 상태전이분석, 모델기반 침입탐지 방법등으로 구분된다.

비정상적인 행위 탐지방법은 시스템 또는 사용자가 정상적인 행위로부터 벗어나는 것을 탐지하는 것으로, 시스템 또는 사용자의 정상행위를 기록한 감사데이터로부터 여러가지 방법을 통해 정상행위를 수집한 후 수행되는 시스템의 행위가 정상행위로부터 벗어나면 경고를 발생한다. 즉, 비정상적인 행위 탐지방법은 전에 학습되지 않은 행위가 시스템에서 발생하면 침입으로 간주한다. 이러한 비정상적인 행위를 탐지하는 대표적인 방법은 통계적 접근방법으로서 사용자나 시스템이 실행시킨 프로세스의 행위를 관찰하고, 각각의 행위에 대한 프로파일을 생성한다. 이때 프로파일을 구성하는 행위의 특징으로는 세션의 로그인과 로그아웃 시간, 세션동안 프로세서, 메모리, 디스크 자원의 사용량 등이다. 이처럼 정상행위 프로파일을 구성한 후 사용자 및 시스템의 행위가 기설정된 정상행위로부터 벗어나는지를 판단한다. 이외에도 비정상행위를 탐지하는 방법으로는 전문가시스템, 신경망, 예측 가능한 패턴 생성방법, 사용자 중심 접근방법 등이 있다.

한편, 네트워크 기반의 침입탐지시스템(NIDS: Network-based IDS)은 주로 네트워크 패킷이나 SNMP MIB, 응용 프로그램 로그 등을 분석하여 침입을 탐지한다. NIDS는 네트워크 기반의 공격을 탐지하여 네트워크 기반 구조를 보호하고자 하는 것이 목적인 만큼 대부분의 경우 호스트 기반 침입 탐지시스템에서 처럼 특정 호스트의 공격은 탐지하거나 상세한 기록을 남길 수 없다. NIDS는 또한 모든 트래픽의 실시간 분석을 통해 침입을 탐지해야 하는데, 네트워크의 고속화에 비례하여 대용량의 트래픽을 실시간으로 분석하기 위해서는 패킷 캐쳐 성능을 향상시킬 필요가 있다.

그리고 네트워크 기반 침입탐지시스템(NIDS)은 대부분 네트웍접속카드(NIC)를 통해 네트워크 패킷을 수집하여 수동분석(Passive Analysis)을 하기 때문에 기존의 네트워크 자원에 전혀 오버헤드를 주지 않고 설치가 용이하며, 네트워크 억세스 지점에만 설치하면 전체 네트워크에 대해 처리할 수 있다. 또한 호스트기반과는 달리 네트워크 기반 모니터

들은 능동적으로 프로토콜에 관여하는 일이 없고, 단지 전송되는 패킷을 수집 분석하는 만큼 공격자가 쉽게 억세스할 수 없으며, 따라서 공격자에게 노출되지 않고 침입을 감시할 수 있다.

도 2는 본 발명에 따른 네트워크 기반 침입탐지시스템의 구성을 도시한 블럭도이다.

본 발명에 따른 네트워크 기반 침입탐지시스템은 통상의 호스트들이 연결되어 패킷이 전송되는 내부망(120)과, 내부망에 연결되어 내부망의 모든 패킷을 캡쳐링하는 침입탐지 센서(IDS 센서)(200)와, IDS 센서(200)에서 검출된 패킷을 분석하여 침입을 판정하고 조치하는 IDS 서버(280)로 구성된다. 특히, 본 발명의 실시예에서 IDS서버(280)는 N개의 IDS서버들(280-1~280-n)이 로드 세어링(load sharing) 방식의 분산구조로 연결되어 IDS망(270)을 형성함으로써 침입분석 성능을 향상시킬 수 있도록 되어 있다. 따라서 침입탐지 센서(200)로부터 수집된 패킷들은 N개의 IDS서버(280-1~280-n)에 적절하게 분산되어 전달된다. 이 때 각 IDS 서버(로 전달되는 패킷들은 패킷 필터링을 거친 후 전달될 수도 있다.

도 2를 참조하면, 침입탐지 센서(200)는 패킷 수집 및 분배부(210)와, 제1 버퍼링부(220), 패턴 매칭부(230), 패킷 필터링 및 분해부(240), 제2 버퍼링부(250), 분배부(260)로 구성되어 크게 패킷을 감지하는 기능과 수신된 패킷을 분석하는 기능, 로드 세어링 방식으로 분산 IDS망(270)으로 패킷을 분배하는 기능을 처리한다.

패킷 수집 및 분배부(210)는 IP를 갖지 않는 MPC860 이더넷 칩(212)으로 구현되어 내부망(120)의 패킷을 수집하여 제1 버퍼링부(220)로 분배하고, 제1 버퍼링부(220)는 복수개의 듀얼포트 램(Dual-port RAM:222)으로 구현된다. 패턴 매칭부(230)는 제1 버퍼링부(220)가 출력하는 패킷들을 미리 내장된 패턴과 비교하여 하드웨어적으로 오용 침입을 탐지한다. 이러한 패턴 매칭부(230)는 다수의 필드 프로그래머블 게이트 어레이(FPGA:232)로 구현된다.

패킷 필터링 및 분해부(240)는 MC68302 마이콤(242)으로 구현되어 패킷을 분해한 후 부하 상태를 고려하여 적절히 분배한다. 제2 버퍼링부(250)는 듀얼포트램(Dual-port RAM: 252)으로 구현되어 IDS 서버(280)로 전달할 분해된 패킷을 일시 저장하고, 분배부(250)는 MPC860 이더넷 칩(262)으로 구현되어 제2 버퍼링부(250)의 출력을 IDS망(270)을 통해 IDS 서버(280-1~280-n)로 전달한다.

각 IDS 서버(280-1~280-n)는 전달된 패킷을 분석하여 각 IP별로 정상 프로파일을 생성하여 비정상 행위를 탐지한다. 그리고 패턴 매칭과 패킷 분석에 의해 침입이 탐지되면 보안 관리자(네트워크 관리자)에게 이를 통지한다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 따른 네트워크 기반 침입탐지 시스템은 하드웨어 기반의 패턴 매칭을 이용하므로 고속망에서 작은 사이즈의 패킷도 상실(lost)하지 않고 캐쉬할 수 있으므로 패킷 캐쉬(packet capture) 성능을 100% 에 가깝게 향상시킬 수 있고, 이에 따라 망에서의 오용 탐지 성능과 비정상 행위를 신속 정확하게 탐지할 수 있는 잇점이 있다. 특히, 내부망에 IP없이 접속되어 수동적으로 모든 패킷을 캐쉬한 후 분석하므로 침입자에게 노출될 염려가 없고, 침입이 탐지되면 IDS 서버에 의해 네트워크 관리자에게 전자메일이나 통신수단을 통해 신속하게 전달함과 아울러 적절하게 대응할 수 있는 잇점이 있다.

(57) 청구의 범위

청구항 1.

망에 접속되어 패킷을 수집한 후 침입을 탐지하는 네트워크 기반 침입탐시스템에 있어서,

상기 망에 접속되어 패킷을 수집한 후 패턴매칭을 통해 오용을 탐지하는 침입탐지 센서; 및

상기 침입탐지 센서로부터 수집된 패킷을 수신하여 각 소스별 정상 프로파일을 생성하고 비정상 행위를 탐지하는 침입탐지 서버를 구비하는 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 2.

제1항에 있어서, 상기 침입탐지 센서는

망으로부터 패킷을 수집하여 분배하는 패킷수집 및 분배부와; 미리 패턴을 저장하고 있다가 상기 패킷 수집 및 분배부로부터 전달된 패킷과 비교하여 침입을 감지하는 패턴 매칭부; 상기 패턴 매칭부로부터 전달된 패킷을 분해하는 패킷 필터링 및 분해부; 및 상기 패킷 필터링 및 분해부로부터 전달된 데이터를 상기 침입탐지 서버로 전달하기 위한 분배부를 포함하는 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 3.

제2항에 있어서, 상기 패턴매칭부는 FPGA로 구현되는 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 4.

제2항에 있어서, 상기 침입탐지 센서는

상기 패킷 수집 및 분배부의 출력을 일시 저장하기 위한 제1 버퍼링부를 더 구비한 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 5.

제2항에 있어서, 상기 침입탐지 센서는

상기 패킷 필터링 및 분해부의 출력을 일시 저장하기 위한 제2 버퍼링부를 더 구비한 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 6.

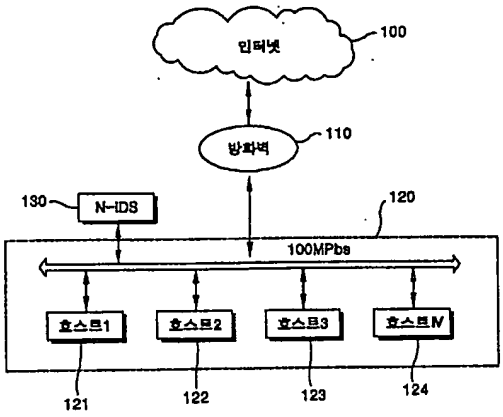
제1항에 있어서, 상기 침입탐지 서버는 이더넷을 통해 연결된 부하 분산망으로 구현된 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

청구항 7.

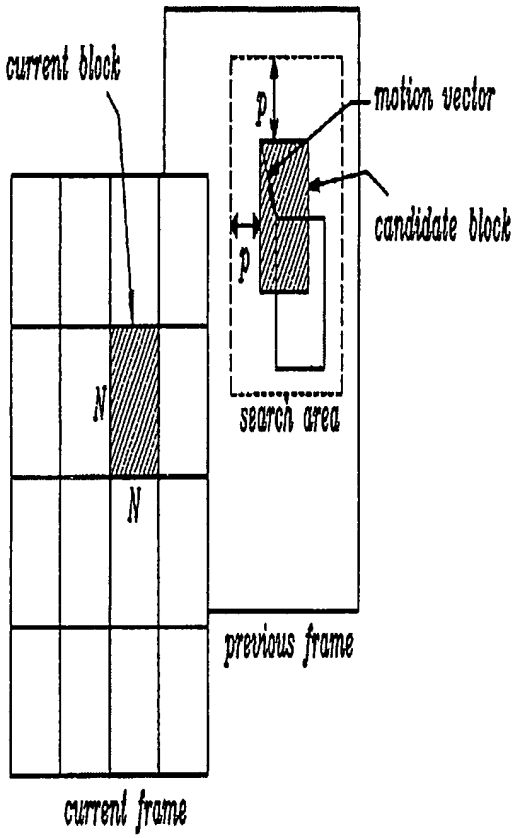
제1항에 있어서, 상기 침입탐지 서버는 침입이 탐지되면 그 내용을 데이터베이스에 저장하고 네트워크 관리자에게 통지하는 것을 특징으로 하는 네트워크 기반 침입탐지 시스템.

도면

도면 1


인터넷
100
방화벽
110
130
N-IDS
120
100MPbs
호스트1
호스트2
호스트3
호스트M
121
122
123
124

도면 2


current block
motion vector
candidate block
p
p
N
N
search area
previous frame
current frame